FortiAuthenticator™ 2.0 MR2 Patch Release 3

Release Notes

FortiAuthenticator™ 2.0 MR2 Patch Release 3 Release Notes

October 22, 2013

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction

This document provides a summary of support information, installation instructions, integration, resolved and known issues in FortiAuthenticator v2.0 MR2 Patch Release 3 build 0210. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiAuthenticator device, see the FortiAuthenticator Administration Guide.

FortiAuthenticator 2.0 MR2 Patch Release 3 does not deliver any additional functionality over the previous patch release. The purpose of this release is to increase the firmware partition size on FortiAuthenticator-VM installs only prior to upgrade from FortiAuthenticator 2.0 MR2 (and lower) to FortiAuthenticator 3.0.

Due to the default firmware partition size being too small to accommodate the expanded firmware, FortiAuthenticator-VM does not support upgrade from FortiAuthenticator 2.0 MR2 PR2 and lower directly to FortiAuthenticator 3.0. To enable upgrade from FortiAuthenticator 2.0 MR2 (including PR1 and PR2), an interim upgrade step via FortiAuthenticator™ 2.0 MR2 Patch Release 3 is required.

To upgrade, use the Firmware Upgrade Process below to upgrade initially to FortiAuthenticator 2.0 MR2 Patch Release 3 (build 210), then repeat the process to upgrade to FortiAuthenticator 3.0 ensuring to backup the firmware at each step.

For additional documentation, please visit:

http://docs.fortinet.com/fauth.html

Supported models

The following models are supported by FortiAuthenticator™ 2.0 MR2 Patch Release 3.

FortiAuthenticator 200D*

FortiAuthenticator 400C*

FortiAuthenticator 1000C*

FortiAuthenticator 3000B*

FortiAuthenticator-VM

*** Whilst it is supported, it is not necessary to upgrade hardware appliances to this release before upgrading to FortiAuthenticator 3.0.**

Special Notices

TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the Web-based Manager to be viewed properly without need for scrolling.

Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. *Go to System* > *Maintenance* > *Config* and select *Download Backup File* to backup the configuration.

After any upgrade

If you are using the Web-based Manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the Web-based Manager screens are displayed properly

Downgrading

If downgrading FortiAuthenticator from 3.0 to a prior release, due to a change in the Session Cookie format, login will fail. Before attempting to login following downgrade, clearing the browser cache will avoid this issue.

Upgrade instructions

Back up your configuration before beginning this procedure. Whilst no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Upgrading from previous releases –VM releases only

Do not upgrade FortiAuthenticator virtual machine appliances directly from v.2.0 MR2 PR2 and lower to v.3.0. **This will result in data loss.** Please follow the procedure below.

To upgrade, use the Firmware Upgrade Process below to upgrade initially to FortiAuthenticator™ 2.0 MR2 Patch Release 3 (build 210), then repeat the process to upgrade to FortiAuthenticator 3.0 ensuring to backup the firmware at each step.

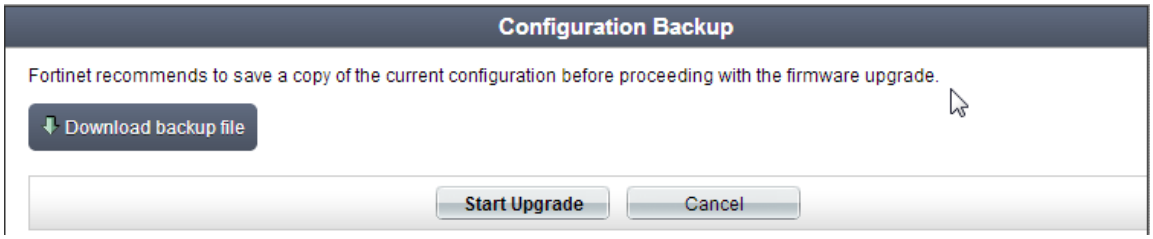
Firmware upgrade process

After backing up your configuration first, follow the following procedure to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware package from the Customer Service & Support web site, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Customer Service & Support web site at https://support.fortinet.com. In the Download section of the page, select the Firmware Images link to download the firmware.
2. To verify the integrity of the download, go back to the Download section of the login page, then click the *Firmware Image Checksums* link.
3. Log in to the FortiAuthenticator unit's Web-based Manager using the *admin* administrator account.
4. Go to *System* > *Dashboard* > *Status*.
5. In the *System Information* widget, in the *Firmware Version* row, select *Upgrade*. The *Firmware Upgrade* or *Downgrade* dialog box opens.
6. In the *Firmware* section, select *Choose File*, and locate the upgrade package that you downloaded.
7. Select *OK* to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



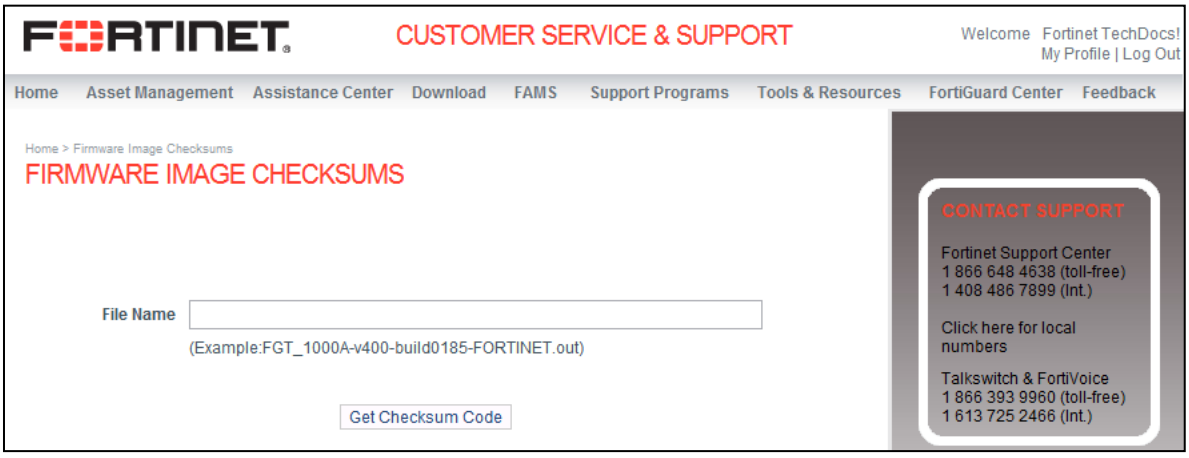
It is recommended that a system backup is taken at this point. Once complete, click ***Start Upgrade.***

Wait until the unpacking, upgrade and reboot process completes (usually 3-5 minutes), then refresh the page.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, go to *Download* > *Firmware Image Checksums*. In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.



Product Integration and Support

Web browser support

The following web browsers are supported by FortiAuthenticator v2.0 MR2:

- Microsoft Internet Explorer versions 8 to 10
- Mozilla Firefox versions 15 to 17
- Google Chrome versions 22 to 29

Other web browsers may function correctly, but are not supported by Fortinet.

Virtualization software support

FortiAuthenticator 2.0 MR2 PR3 supports VMware ESXi / ESX 4.0, 4.1, 5.0 and 5.1.

See Appendix A: FortiAuthenticator VM for more information.

Third party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS). For more information, see the FortiAuthenticator Two-Factor Authentication Interoperability Guide http://docs.fortinet.com/fauth.html

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
217365	Firmware upgrade from 2.0 to 3.0 fails for VM models

Known Issues

There are no known issues reported with FortiAuthenticator v2.0 MR2 Patch Release 3 build 0210. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Appendix A: FortiAuthenticator VM

FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator VM system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported virtual machine (VM) environment. For details, see the Install Guide for FortiAuthenticator VM available at http://docs.fortinet.com.

Table 2: VM Requirements

Virtual Machine	Requirement
Hypervisor Support	VMware ESXi / ESX 4.0, 4.1, 5.0 and 5.1
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Virtual CPUs Supported (Minimum / Maximum)	1 / 8
Virtual NICs Supported (Minimum / Maximum)	1 / 4
Storage Support (Minimum / Maximum)	60GB / 2TB
Memory Support (Minimum / Maximum)	512 MB / 4GB
High Availability Support	Yes

FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- ***.out:*** Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- ***ovf.zip***: Use this image for new VM installations. It contains a deployable Open Virtualization Format (OVF) virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortiauthenticator/index.html